



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/679,186

10/03/2003

Fred Cohen

529-000210US

9775

22798 7590 04/03/2007
QUINE INTELLECTUAL PROPERTY LAW GROUP, P.C.
P O BOX 458
ALAMEDA, CA 94501

EXAMINER

SMITHERS, MATTHEW

ART UNIT

PAPER NUMBER

2137

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
--	-----------	---------------

3 MONTHS

04/03/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/679,186

Applicant(s)

COHEN ET AL.

Examiner

Matthew B. Smithers

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address.

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 October 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 03 October 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.104(a).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 11/08/04.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed November 8, 2004 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Objections

Claim 32 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 32 recites "A stored program product on a media . . . to perform the method of claim 20". Claim 32 does not limit the subject matter of method claim 20. Therefore, it should be rewritten as an independent claim within the meaning of 35 USC 101 or written as a proper dependent claim.

Specification

The disclosure is objected to because of the following informalities: In the cross reference to applications section the application number of the last case is missing.

Appropriate correction is required.

The attempt to incorporate subject matter into this application by reference to embedded hyperlinks, see page 3 of applicant's specification, is ineffective because the incorporation is not in accordance with 37 CFR 1.57(d) and MPEP § 608.01(p), paragraph I.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 3-19, 32 and 33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. With respect to claim 3, the claim recites "A computer program product . . . comprising: a computer useable medium having computer readable program code embodied therein, said computer program product further comprising: . . . ". In reviewing the specification it is clear the computer useable medium can be either in the form of a fixed media or through a transmissible program component (see paragraph [0196] of applicant's specification). Transmissible program components do not fall within one of the four statutory classes of an invention. The transmissible program components lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101, it is clearly not a series of steps to a process (method) and it is not a combination of chemical compounds to be a composition of matter. As such, the transmissible program components fail to fall within a statutory category. Claims 4-19 and 33 each depend

Art Unit: 2137

from claim 3 and all fail to provide the necessary elements needed to meet 35 USC 101 as explained above.

With respect to claim 32, the claim recites "A stored program product on a media . . . to perform the method of claim 20". In reviewing the specification it is clear the media can be either in the form of a fixed media or through a transmissible program component (see paragraph [0196] of applicant's specification). Transmissible program components do not fall within one of the four statutory classes of an invention. The transmissible program components lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101, it is clearly not a series of steps to a process (method) and it is not a combination of chemical compounds to be a composition of matter.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-13 and 15-33 are rejected under 35 U.S.C. 102(e) as being ~~art~~ by U.S. patent 6,907,533 granted to Sorkin et al.

Regarding claim 1, Sorkin meets the claimed limitations as follows:

Art Unit: 2137

“A method of operating an information appliance comprising: receive a logic request at an operating system; determine if a deception should be provided by the operating system; if yes, do one or more of:
perform a deception action; provide a deception response; fulfill said logic request;
if no fulfill the request normally.” see column 14, line 37 to column 16, line 4.

Regarding claim 2, Sorkin meets the claimed limitations as follows:

“A method of operating an information appliance comprising: receive a logic request at an operating system; determine if communication with external logic is desired; if yes: using external logic, determine if deception will be performed by the operating system; using external logic, decide what deception is to be performed; perform a deception action; optionally provide a deception response; optionally fulfill said logic request action; if no: evaluate and fulfill said logic request.” see column 14, line 37 to column 16, line 4.

Regarding claim 3, Sorkin meets the claimed limitations as follows:

“A computer program product for use in an information system comprising:

a computer useable medium having computer readable program code embodied therein, said computer program product further comprising:

computer readable program code enabling a loadable kernel module able to intercept system calls;

wherein said kernel module, after intercepting a system call, grants, refuses to grant, or falsifies granting or refusing said system call depending on one or more parameters of a system call and/or an entity making said system call; and wherein said

Art Unit: 2137

kernel module, after intercepting a system call, returns either an accurate or an inaccurate response to said system call depending on one or more parameters of a system call and/or an entity making said system call.” see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 4, Sorkin meets the claimed limitations as follows:

“The computer program product of claim 3 further wherein: said kernel module comprising a control module and one or more decision modules.” see column 16, lines 28-47 and Figure 11.

Regarding claim 5, Sorkin meets the claimed limitations as follows:

“The computer program product of claim 3 further wherein: said kernel module can selectively return false responses in response to system calls.” see column 22, lines 3-25 and Figures 17-34.

Regarding claim 6, Sorkin meets the claimed limitations as follows:

“The computer program product of claim 3 further wherein: said kernel module can probabilistically return false responses in response to system calls.” see column 8, lines 5-15 and Figure 4.

Regarding claim 7, Sorkin meets the claimed limitations as follows:

“The computer program product of claim 3 further comprising: computer readable program code that when loaded into an appropriately configured information system provides a control mechanism able to identify, mark, and control deceptions provided in

Art Unit: 2137

response to system calls." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 8, Sorkin meets the claimed limitations as follows:

"The computer program product of claim 3 further wherein: said kernel module intercepts all system calls." see column 22, lines 3-25 and Figures 17-34.

Regarding claim 9, Sorkin meets the claimed limitations as follows:

"The computer program product of claim 3 further wherein: said kernel module intercepts one or more system calls analogous to: open(); read(); chdir(); stat64(); lstat64(); setuid(); setgid(); setgroups32(); getdents64(); write(); unlink(); rmdir(); getuid32(); getgid32(); geteuid32(); getegid32(); getgroups32(); chmod(); rename(); mkdir(); delete_module(); or socketcall()." see column 24, line 65 to column 25, line 65 and Figures 17-34.

Regarding claim 10, Sorkin meets the claimed limitations as follows:

"The computer program product of claim 3 further wherein: said control module intercepts four or more system calls analogous to: open(); read(); chdir(); stat64(); lstat64(); setuid(); setgid(); setgroups32(); getdents64(); write(); unlink(); rmdir(); getuid32(); getgid32(); geteuid32(); getegid32(); getgroups32(); chmod(); rename(); mkdir(); delete_module(); or socketcall()." see column 24, line 65 to column 25, line 65 and Figures 17-34.

Regarding claim 11, Sorkin meets the claimed limitations as follows:

"The computer program product of claim 3 further comprising: a user space interface allowing changes in deception behavior to be made while said kernel module is

inserted.” see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 12, Sorkin meets the claimed limitations as follows:

“The computer program product of claim 3 further comprising: a module able to simulate/procflesystem type system call.” see column 14, line 37 to column 16, line 4; and Figure 10.

Regarding claim 13, Sorkin meets the claimed limitations as follows:

“The computer program product of claim 3 further wherein said control module can transparently cause deceived processes to access different storage and processing areas or systems during a system call.” see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 15, Sorkin meets the claimed limitations as follows:

“An information processing system comprising logic processing apparatus and operating system central logic comprising: a caller identifier able to indicate calling entities for deception; one or more system calls able to set said caller identifier to mark a calling entity for deception; and one or more system calls able to read said caller identifier and able to provide deceptive responses and/or take deceptive actions when called by an entity marked for deception.” see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 16, Sorkin meets the claimed limitations as follows:

Art Unit: 2137

"The system of claim 15 further wherein: said one or more system calls are able to provide deceptive responses and/or take deceptive actions probabilistically." see column 8, lines 5-15 and Figure 4.

Regarding claim 17, Sorkin meets the claimed limitations as follows:

"The system of claim 15 further wherein: said one or more system calls are able to provide deceptive responses and/or take deceptive actions selectively." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 18, Sorkin meets the claimed limitations as follows:

"The system of claim 15 further wherein: said one or more system calls evaluate one or more system and/or user parameters in determining whether to or how to select to provide deceptive responses or take deceptive actions." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 19, Sorkin meets the claimed limitations as follows:

"The system of claim 15 further comprising: a user space interface allowing changes in deception behavior of one or more system calls to be made during operation of said operating system central logic." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 20, Sorkin meets the claimed limitations as follows:

"A method of modifying operation of an information system comprising:
initiating a requested operating system call; deciding among three or more possible responses to said system call; wherein said responses comprise an accurate or an inaccurate response to a system call; and wherein said responses further comprise granting, refusing to grant, or falsifying granting or refusing said system call." see column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 21, Sorkin meets the claimed limitations as follows:

"The method of claim 20 further wherein said responses further comprise modifying said system call request prior to executing said system call." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 22, Sorkin meets the claimed limitations as follows:

"The method of claim 20 further wherein said responses further comprise undetectably redirecting said system call to be performed in another information processing environment." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 23, Sorkin meets the claimed limitations as follows:

"The method of claim 20 further comprising: selectively returning false responses to system calls:" see column 22, lines 3-25 and Figures 17-34.

Regarding claim 24, Sorkin meets the claimed limitations as follows:

"The method of claim 20 further comprising: probabilistically returning false responses to system calls." see column 8, lines 5-15 and Figure 4.

Art Unit: 2137

Regarding claim 25, Sorkin meets the claimed limitations as follows:

"The method of claim 20 further comprising: identifying, marking, and controlling deceptions provided in response to system calls through a user space interface." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 26, Sorkin meets the claimed limitations as follows:

"The method of claim 20 further comprising: intercepting all system calls by system call control logic." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 27, Sorkin meets the claimed limitations as follows:

"The method of claim 20 further comprising: transparently changing deceived processes to access different storage and processing areas or systems during a system call." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 28, Sorkin meets the claimed limitations as follows:

"A method of defending an information processing system from possibly undesired operations comprising: initiating an operating system call; deciding among a set of possible responses to said system call; and wherein said set of possible responses comprises accurate and inaccurate responses." see column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 29, Sorkin meets the claimed limitations as follows:

Art Unit: 2137

"A method of defending an information processing system from intentional and/or unintentional destructive operations comprising: intercepting an operating system; deciding among a set of possible responses to said system call; and wherein said set of possible responses comprises granting, refusing to grant, falsifying granting or refusing, and modifying execution of said system call." see column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 30, Sorkin meets the claimed limitations as follows:

"The method of claim 29 further wherein: said set of possible responses comprises performing a requested call in a different information processing environment." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 31, Sorkin meets the claimed limitations as follows:

"A method of enhancing security in an information processing comprising: modifying two or more system calls to identify entities for deception and/or provide deception functions; and providing deceptions from a system call to an entity identified for deception." see column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Regarding claim 32, Sorkin meets the claimed limitations as follows:

"A stored program product on a media that when loaded and executed in an appropriately configured computer device enables the device to perform the method of claim 20." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Art Unit: 2137

Regarding claim 33, Sorkin meets the claimed limitations as follows:

"A stored program product on a media that when loaded and executed in an appropriately configured computer device enables the device to embody the system of claim 3." see column 7, line 4 to column 9, line 16; column 11, lines 33-51; column 14, line 37 to column 16, line 4; column 22, lines 4-65 and Figures 17-34.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Teal et al (US 20030120935) discloses a kernel-based network security infrastructure.

B. Kedma et al (US 20020099954) discloses a method for detecting breaches in operating systems.

C. Schlossberg et al (US 20020066034) discloses a network security deception system.

D. Pham et al (US 7,143,288) discloses a method for controlling access to a security file system.

E. Sheymov (US 7,010,698) discloses a method for creating a code inspection system.

F. O'Brien et al (US 6,58,571) discloses kernel based security framework.

G. Hollander et al (US 6,412,071) discloses a method for detecting illegal attempts a computing environment.

H. Yarom (US 5,956,710) discloses a method for providing user exits on an operating system platform.

I. Hsu (US 5,584,023) discloses a secure file transform used for controlling file manipulations.

J. Arnold et al (US 5,440,723) discloses an automatic immune system for computers and networks.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

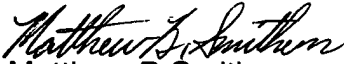
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/679,186

Page 15

Art Unit: 2137

A handwritten signature in black ink, reading "Matthew B. Smithers". The signature is written in a cursive style with a large, stylized "M" and "S".

Matthew B Smithers

Primary Examiner

Art Unit 2137